Guest Editors Introduction: Special Issue on Network-on-Chip Architectures of the Future (NoCArc)

As the number of cores integrated into the same integrated circuit increases, the role of the Network-on-Chip (NoC)—as the communication infrastructure—becomes increasingly more important. Next-generation many-core processor systems continue to face communication-related scalability problems, which are further exacerbated by ultra-deep sub-micron effects induced by the next silicon technology nodes. The emergence of novel computing paradigms consisting of accelerators, quantum computing, DNA computing storage technologies, and optical computing can have deep and far-reaching implications on the future of interconnects. Integration platforms such as interposers and processing-in-memory are also predicted to influence the course of NoC research. Furthermore, applications such as big data, artificial intelligence, deep learning, and cybersecurity will also impact the future of NoC research.

With the end of Dennard scaling, large many-core processor systems are disaggregated into smaller chiplets or dielets and are integrated using traditional platforms such as boards as well as emerging technologies such as 2.5D interposers, Silicon Photonics (SiPh), or wireless interconnects. Interposers are large silicon dies with minimum or no active devices providing abundant wiring resources to interconnect dielets integrated on sockets in the interposer. The capability to reuse older more mature technology nodes due to minimum active devices and the use of only long-distance global wire-based interconnects make interposers a natural choice for low-cost and sustainable scalable platforms that do not need new materials and can reuse existing fabrication nodes. The abundant wiring resources provide new opportunities for scaling the number of chiplets in the system and for research into novel, application-informed Network-in-Package (NiP) designs that provide designers a wide range of tradeoffs in performance, energy efficiency, reliability, scalability, and sustainability.

SiPh is maturing as an on-chip and chip-to-chip interconnect technology. Using miniature ring resonators, Mach-Zehnder modulator/demodulators, and waveguides, dense wavelength division multiplexing is supported where multiple pairs of senders and receivers can communicate with high bandwidth over chip-side dimensions with ultra-low latency and improved energy efficiency. Integration and miniaturization of the SiPh devices at larger densities and elimination of electro-optic domain conversions remain open challenges in this field.

Wireless and radio frequency communication among cores in a many-core system over NoC or NiP links can provide latency-bound communication using miniature millimeter-wave or sub-THz bands over multi-gigabit per second links. Wireless communication provides support for broadcast or multicast traffic, which is extremely beneficial in many-core processor systems due to essential control messages such as cache coherency protocol messages. By eliminating repeated unicasts,

ACM Reference format:
Amlan Ganguly, Salvatore Monteleone, Diana Goehringer, and Cristinel Ababei. 2023. Guest Editors Introduction: Special Issue on Network-on-Chip Architectures of the Future (NoCArc). *ACM J. Emerg. Technol. Comput. Syst.* 19, 3, Article 19 (July 2023), 3 pages.
https://doi.org/10.1145/3609500

1550-4832/2023/07-ART19
https://doi.org/10.1145/3609500

the performance of many-core platforms with multi-level caches can improve significantly. However, wireless interconnects introduce new challenges pertaining to security and data integrity. Due to transmissions over unguided media, physical jamming and eavesdropping scenarios are conceivable by attackers in close proximity to the systems. Therefore, smart wireless communication protocol designs capable of providing necessary performance and security features remain open challenges in this area.

NoCs and NiPs occupy significant real estate and therefore offer a large surface area for several kinds of attack vectors. These include denial-of-service, sinkhole, blackhole, data corruption, and even different kinds of side-channel attacks. Traditional methods such as firewalls and OS or hypervisor-level protections are not sufficient to address hardware vulnerabilities, as these can be exploited through complex multi-agent attacks. Novel and zero-day security attacks and their appropriate defense strategies remain open challenges in this space.

Multi/many-core, disaggregate multi-chiplet, or dielet-based systems integrated with an NoC or NiP offer an open design space if application-based co-design or application-informed design is considered. Novel topologies, communication protocols, and routing, security, and reliability methods remain exciting research dimensions in the area of NoC (or NiP) architectures. With the emergence of machine learning and deep learning, along with advancement in neural network designs, NoC/NiP design is poised to undergo major revolutions. For example, the use of machine learning for NoC architecture design is an attractive design direction. Design of NoC or NiP based systems for deep learning applications and emerging hyperscale artificial intelligence applications are also exciting new research directions. Within this context, this special issue on NoC architectures of the future includes four articles proposing cutting-edge research ideas in this domain.

The first article, "Machine Learning Enabled Solutions for Design and Optimization Challenges in Networks-on-Chip Based Multi/Many-Core Architectures" authored by Md. Farhadur Reza, explores the use of a neural network based machine learning framework for exploring NoC architecture design space and proposes optimized architectures. Simulation results show that the performance of a neural network based optimal solution results in 15% performance and 6% energy consumption improvement.

The second article,"2DMAC: A Sustainable and Efficient Medium Access Control Mechanism for Future Wireless NoCs" authored by Sidhartha Rout et al., proposes a novel medium access control protocol (MAC) for wireless NoCs that improves interference avoidance. By using a priority-based channel sharing mechanism, the proposed solution can improve data transfer throughput and critical message latency by nearly 30%.

The third article, "Characterization of Timing-Based Software Side-Channel Attacks and Mitigations on Network-on-Chip Hardware" authored by Usman Ali et al., investigates the possibility of side-channel attacks through the NoC. The article shows that up to 97% attack efficacy is achievable even in the presence of noise. Additionally, the article shows that isolation schemes can achieve defense against such attacks with a low 2% to 3% impact on performance.

The fourth article, "Securing Network-on-Chips Against Fault-Injection and Crypto-Analysis Attacks via Stochastic Anonymous Routing" authored by Ahmad Patooghy et al., discusses how unencrypted or partially encrypted message exchange over the NoC can reveal sensitive information and expose security vulnerabilities of the system to an attacker. In this article, the authors propose a stochastic routing approach that defends the NoC against such attacks for a low area and 20% power overheads.

We believe that this special issue captures a cross section of important, interesting, and exciting research in the fields of NoC and NiP. The articles, authored by expert authors and scientists in the area, represent the state of the art in research at the time of publication of this issue. For any questions, readers are encouraged to contact the communicating authors of the respective articles.

Amlan Ganguly
Computer Engineering, Rochester Institute of Technology, USA
axgeec@rit.edu

Salvatore Monteleone
Department of Engineering, Niccolò Cusano University, Italy
salvatore.monteleone@unicusano.it

Diana Goehringer
Technische Universität Dresden, Germany
diana.goehringer@tu-dresden.de

Cristinel Ababei
Electrical and Computer Engineering, Marquette University, USA
cristinel.ababei@marquette.edu

Guest Editors